Finite Fields and Their Applications **8,** 491–503 (2002)
doi:10.1006/ffta.2002.0358

On the Average Distribution of Inversive Pseudorandom Numbers

Harald Niederreiter

Department of Mathematics, National University of Singapore, 2 Science Drive 2, Singapore 117543, Republic of Singapore
E-mail: nied@math.nus.edu.sg

and

Igor E. Shparlinski

Department of Computing, Macquarie University, NSW 2109, Australia
E-mail: igor@comp.mq.edu.au

Communicated by Peter Jau-Shyong Shiue

Received August 13, 2001; revised February 17, 2002; published online May 28, 2002

The inversive congruential method is an attractive alternative to the classical linear congruential method for pseudorandom number generation. The authors have recently introduced a new method for obtaining nontrivial upper bounds on the multidimensional discrepancy of inversive congruential pseudorandom numbers in parts of the period. This method has also been used to study the multidimensional distribution of several other similar families of pseudorandom numbers. Here we apply this method to show that, "on average" over all initial values, much stronger results than those known for "individual" sequences can be obtained. © 2002 Elsevier Science (USA)

Key Words: pseudorandom numbers; discrepancy; inversive congruential generator; digital inversive generator.

1. INTRODUCTION

Let q be a (large) prime power and let $\mathbb{F}_q$ be the field of q elements. For given $\alpha \in \mathbb{F}_q^*$, $\beta \in \mathbb{F}_q$, let ψ be the permutation of $\mathbb{F}_q$ defined by

$$\psi(\gamma) = \begin{cases} \alpha\gamma^{-1} + \beta & \text{if } \gamma \neq 0, \\ \beta & \text{if } \gamma = 0. \end{cases} \tag{1}$$

1071-5797/02 $35.00

Let $u_0(\vartheta), u_1(\vartheta), \ldots$ be the sequence of elements of $\mathbb{F}_q$ obtained by the recurrence relation

$$u_{n+1}(\vartheta) = \psi(u_n(\vartheta)), \qquad n = 0, 1, \ldots, \tag{2}$$

where $u_0(\vartheta) = \vartheta$ is the *initial value*. It is obvious that the sequence (2) is purely periodic with some least period $t \le q$. It is known when such sequences achieve the largest possible period $t = q$ (see [1, 9, 21]).

Two types of sequences of pseudorandom numbers can be derived from the sequence (2): *inversive congruential pseudorandom numbers* (see Section 3) where q is a prime p and *digital inversive pseudorandom numbers* (see Section 4) where q is a power of a small prime.

The inversive congruential generator provides a very attractive alternative to linear congruential generators and has been extensively studied in the literature. For sequences of inversive congruential pseudorandom numbers of period $t = p$, a number of results about the distribution and statistical almost-independence of inversive congruential pseudorandom numbers over the full period have been established, starting with the paper [18]. Many of these results are essentially best possible. We refer to [5–7, 17–20, 22, 23] for more details and references to original papers.

In [27], we introduced a method which allowed us to give the first nontrivial bounds on the one-dimensional discrepancy of an individual sequence of inversive congruential pseudorandom numbers in parts of the period. In [14], this method was extended to the multidimensional discrepancy. In [24], similar results were obtained for sequences satisfying the relation $u_{n+1}(\vartheta) = f(u_n(\vartheta))$ with a polynomial $f(X) \in \mathbb{F}_p[X]$. In the series of papers [12–14, 23, 25, 26, 29–31], this method was successfully applied to many other similar generators; see also the recent survey [28] and the paper [2] where the method is analyzed in the more general setting of arbitrary finite abelian groups.

In the very special but important case for cryptographic applications where $f(X) = X^e$, that is, for the *power generator*, alternative approaches have been proposed in [10, 11]. These approaches, although they have produced quite strong results for the power generator, cannot be extended to other nonlinear generators.

In this paper we show that our method can also be used to produce new results on the multidimensional distribution of inversive congruential and digital inversive pseudorandom numbers for all initial segments of length N, starting with very small values of N, when the initial value of the generator is selected at random.

Throughout the paper, the implied constants in the symbols "O" and "$\ll$" may occasionally, where obvious, depend on some integer parameter

$s \geq 1$ and are absolute otherwise (we recall that $A \ll B$ is equivalent to $A = O(B)$).

2. AUXILIARY RESULTS

Let us consider the following sequence of rational functions over $\mathbb{F}_q$:

$$R_0(X) = X, \qquad R_i(X) = R_{i-1}(\alpha X^{-1} + \beta), \qquad i = 1, 2, \ldots.$$

It is obvious that this sequence is purely periodic. Denote by T the least period. Obviously $T \geq t$. It follows from [26, Lemma 1] that there exist elements $\varepsilon_1, \ldots, \varepsilon_{T-1} \in \mathbb{F}_q$, such that

$$R_i(X) = \frac{(\beta - \varepsilon_i)X + \alpha}{X - \varepsilon_i} \qquad \text{for } 1 \leq i \leq T-1.$$

It suffices to observe that in that lemma we must have $\rho_i \neq 0$ for $1 \leq i \leq T-1$. This implies that for $1 \leq i \leq T-1$ we have

$$\psi^i(\gamma) = \frac{(\beta - \varepsilon_i)\gamma + \alpha}{\gamma - \varepsilon_i} \qquad \text{for } \gamma \in \mathbb{F}_q \backslash \{\varepsilon_1, \ldots, \varepsilon_i\}, \tag{3}$$

where ψ^i denotes the ith iterate of the permutation ψ given by (1).

We write

$$\mathbf{e}_m(z) = \exp(2\pi i z/m)$$

for a positive integer m and any integer z. Let χ denote the canonical additive character of $\mathbb{F}_q$, which is given by

$$\chi(\gamma) = \mathbf{e}_p(\mathrm{Tr}(\gamma)) \qquad \text{for all } \gamma \in \mathbb{F}_q,$$

where p is the characteristic of $\mathbb{F}_q$ and Tr is the trace function from $\mathbb{F}_q$ to $\mathbb{F}_p$.

For a vector $\mathbf{h} = (\mu_0, \ldots, \mu_{s-1}) \in \mathbb{F}_q^s$ and integers c, M, N with $M \geq 1$ and $N \geq 1$, we define

$$V_{\mathbf{h},c}(M,N) = \sum_{\vartheta \in \mathbb{F}_q} \left| \sum_{n=0}^{N-1} \chi\left(\sum_{j=0}^{s-1} \mu_j \psi^{n+j}(\vartheta) \right) \mathbf{e}_M(cn) \right|^2.$$

LEMMA 1. *For any prime power q, integers c, M, N with $M \geq 1$ and $1 \leq N \leq T$ and any nonzero vector $\mathbf{h} = (\mu_0, \ldots, \mu_{s-1}\} \in \mathbb{F}_q^s$ we have*

$$V_{\mathbf{h},c}(M,N) \ll A(N,q),$$

where

$$A(N,q) = \begin{cases} Nq & \text{if } N \le q^{1/2}, \\ N^2 q^{1/2} & \text{if } N > q^{1/2}. \end{cases}$$

Proof. We have

$$V_{\mathbf{h},c}(M,N) = \sum_{k,l=0}^{N-1} \mathbf{e}_M(c(k-l)) \sum_{\vartheta \in \mathbb{F}_q} \chi\left(\sum_{j=0}^{s-1} \mu_j(\psi^{k+j}(\vartheta) - \psi^{l+j}(\vartheta))\right)$$
$$\le \sum_{k,l=0}^{N-1} \left| \sum_{\vartheta \in \mathbb{F}_q} \chi\left(\sum_{j=0}^{s-1} \mu_j(\psi^{k+j}(\vartheta) - \psi^{l+j}(\vartheta))\right)\right|.$$

Since ψ is a permutation, the absolute value of the sum over ϑ depends, as a function of k and l, only on $d = |k-l|$. If $d = 0$, then the sum over ϑ is equal to q. Therefore,

$$V_{\mathbf{h},c}(M,N) \le Nq + 2\sum_{d=1}^{N-1} (N-d) \left| \sum_{\vartheta \in \mathbb{F}_q} \chi\left(\sum_{j=0}^{s-1} \mu_j(\psi^{d+j}(\vartheta) - \psi^{j}(\vartheta))\right)\right|.$$

The last sum over ϑ was already considered in [26, Eq. (6)]. Therefore, by the inequality at the bottom of p. 194 in [26] and noting (3), we obtain

$$\left| \sum_{\vartheta \in \mathbb{F}_q} \chi\left(\sum_{j=0}^{s-1} \mu_j(\psi^{d+j}(\vartheta) - \psi^{j}(\vartheta))\right)\right| \le (4s-2)q^{1/2} + 2(d+s-1)$$

provided that $d \le T - s$. Since $d \le N - 1 \le T - 1$, there are at most $s-1$ remaining values of d for which we use the trivial bound q for the above character sum. Hence,

$$V_{\mathbf{h},c}(M,N) \ll Nq + q^{1/2} \sum_{d=1}^{N-1} (N-d) + \sum_{d=1}^{N-1} (N-d)(d+s-1),$$

and after simple calculations we obtain

$$V_{\mathbf{h},c}(M,N) \ll Nq + N^2 q^{1/2} + N^3. \tag{4}$$

We note that the second term in the bound (4) never dominates; thus, we have

$$V_{\mathbf{h},c}(M,N) \ll Nq + N^3.$$

We also remark that because ψ is a permutation, we get for any integer L,

$$\sum_{\vartheta \in \mathbb{F}_q} \left| \sum_{n=L}^{L+N-1} \chi\left(\sum_{j=0}^{s-1} \mu_j \psi^{n+j}(\vartheta) \right) \mathbf{e}_M(cn) \right|^2$$

$$= \sum_{\vartheta \in \mathbb{F}_q} \left| \sum_{n=0}^{N-1} \chi\left(\sum_{j=0}^{s-1} \mu_j \psi^{n+j}(\psi^L(\vartheta)) \right) \mathbf{e}_M(cn) \right|^2 = V_{\mathbf{h},c}(M,N).$$

Therefore, separating the inner sum into at most $N/K + 1$ subsums of length at most K, for any integer $1 \le K \le N$ we have

$$V_{\mathbf{h},c}(M,N) \ll (Kq + K^3)N^2K^{-2} = N^2(qK^{-1} + K).$$

Thus, selecting $K = \min\{N, \lfloor q^{1/2} \rfloor\}$ and taking into account that $qN^{-1} \ge N$ for $N \le q^{1/2}$, we obtain the desired result. ■

We also need the obvious identity

$$\sum_{a=0}^{m-1} \mathbf{e}_m(ab) = \begin{cases} 0 & \text{if } b \not\equiv 0 \pmod m, \\ m & \text{if } b \equiv 0 \pmod m. \end{cases} \tag{5}$$

For integers $m \ge 1$ and c, let us define

$$\|c\|_m = \min_{b \in \mathbb{Z}} |c - bm|.$$

Then we have the easily established inequality

$$\left| \sum_{r=L+1}^{L+Q} \mathbf{e}_m(cr) \right| \le \frac{m}{\max\{1, 2\|c\|_m\}} \tag{6}$$

which holds for any integers c, L, and $m \ge Q \ge 1$.

For a sequence of N points

$$\Gamma = (\gamma_{1,n}, \ldots, \gamma_{s,n})_{n=1}^N \tag{7}$$

of the half-open interval $[0,1)^s$, denote by Δ_Γ its *discrepancy*, that is,

$$\Delta_\Gamma = \sup_{B \subseteq [0,1)^s} \left| \frac{T_\Gamma(B)}{N} - |B| \right|,$$

where $T_\Gamma(B)$ is the number of points of the sequence Γ which hit the box

$$B = [\alpha_1, \beta_1) \times \cdots \times [\alpha_s, \beta_s) \subseteq [0,1)^s$$

and the supremum is taken over all such boxes.

For an integer vector $\mathbf{a} = (a_1, \ldots, a_s) \in \mathbb{Z}^s$ we put

$$|\mathbf{a}| = \max_{j=1,\ldots,s} |a_j|, \qquad r(\mathbf{a}) = \prod_{j=1}^{s} \max\{|a_j|, 1\}. \tag{8}$$

We need the *Erdös–Turán–Koksma inequality* (see [3, Theorem 1.21]) for the discrepancy of a sequence of points of the s-dimensional unit cube, which we present in the following form.

LEMMA 2. *For any integer $G \geq 1$, the discrepancy Δ_Γ of a sequence of points* (7) *satisfies*

$$\Delta_\Gamma \ll \frac{1}{G} + \frac{1}{N} \sum_{0 < |\mathbf{a}| \leq G} \frac{1}{r(\mathbf{a})} \left| \sum_{n=1}^{N} \exp\left(2\pi i \sum_{j=1}^{s} a_j \gamma_{j,n}\right) \right|,$$

where $|\mathbf{a}|, r(\mathbf{a})$ are defined by (8) *and the sum is taken over all integer vectors*

$$\mathbf{a} = (a_1, \ldots, a_s) \in \mathbb{Z}^s$$

with $0 < |\mathbf{a}| \leq G$.

3. DISCREPANCY BOUND FOR INVERSIVE CONGRUENTIAL PSEUDORANDOM NUMBERS

For the generation of inversive congruential pseudorandom numbers we let q be a (large) prime number p and identify the finite field $\mathbb{F}_p$ with the least residue system modulo p. If $u_0(\vartheta), u_1(\vartheta), \ldots$ is the sequence of elements of $\mathbb{F}_p$ generated by (1) and (2) with the initial value $u_0(\vartheta) = \vartheta \in \mathbb{F}_p$, then the numbers $u_0(\vartheta)/p, u_1(\vartheta)/p, \ldots$ in the interval $[0, 1)$ form a sequence of *inversive congruential pseudorandom numbers*. These pseudorandom numbers were introduced by Eichenauer and Lehn [4].

Let $s \geq 1$ be an integer. We denote by $D_N^{(s)}(\vartheta)$ the *s-dimensional discrepancy* of the s-tuples

$$\left(\frac{u_n(\vartheta)}{p}, \frac{u_{n+1}(\vartheta)}{p}, \ldots, \frac{u_{n+s-1}(\vartheta)}{p}\right), \qquad 0 \leq n \leq N-1.$$

We use log to denote the logarithm to the base 2. The number T is defined as in the beginning of Section 2. Let

$$B(N, p, T) = \begin{cases} N^{-1/2} (\log N + 1)^{s+1} \log (T+1) & \text{if } N \leq p^{1/2}, \\ p^{-1/4} (\log N + 1)^{s+1} \log (T+1) & \text{if } N > p^{1/2}. \end{cases}$$

THEOREM 3. *Let $s \ge 1$ be an integer and $0<\varepsilon<1$. Then for all initial values $\vartheta = 0, 1, \ldots, p-1$, except at most $O(\varepsilon p)$ of them, the discrepancy $D_N^{(s)}(\vartheta)$ of inversive congruential pseudorandom numbers satisfies*

$$D_N^{(s)}(\vartheta) \ll \varepsilon^{-1} B(N, p, T) \qquad \text{for } 1 \le N \le T.$$

Proof. Without loss of generality we can assume that $N \ge 2$. From Lemma 2 with $G = \lfloor N/2 \rfloor$ we derive

$$D_N^{(s)}(\vartheta) \ll \frac{1}{N} + \frac{1}{N} \sum_{0<|\mathbf{a}| \le N/2} \frac{1}{r(\mathbf{a})} \left| \sum_{n=0}^{N-1} \mathbf{e}_p\left(\sum_{j=1}^{s} a_j u_{n+j-1}(\vartheta) \right) \right|.$$

Let $m_\nu = 2^\nu$, $\nu = 0, 1, \ldots$, and define $k \ge 1$ by the condition $m_{k-1} < N \le m_k$. From (5) we derive

$$\sum_{n=0}^{N-1} \mathbf{e}_p\left(\sum_{j=1}^{s} a_j u_{n+j-1}(\vartheta) \right) = \frac{1}{m_k} \sum_{n=0}^{m_k-1} \mathbf{e}_p\left(\sum_{j=1}^{s} a_j u_{n+j-1}(\vartheta) \right) \sum_{c=0}^{m_k-1} \sum_{r=0}^{N-1} \mathbf{e}_{m_k}(c(n-r)).$$

Therefore, from (6) we obtain

$$\left| \sum_{n=0}^{N-1} \mathbf{e}_p\left(\sum_{j=1}^{s} a_j u_{n+j-1}(\vartheta) \right) \right| \le \sum_{c=0}^{m_k-1} \frac{1}{\max\{1, 2\|c\|_{m_k}\}} \left| \sum_{n=0}^{m_k-1} \mathbf{e}_p\left(\sum_{j=1}^{s} a_j u_{n+j-1}(\vartheta) \right) \mathbf{e}_{m_k}(cn) \right|.$$

It follows that

$$D_N^{(s)}(\vartheta) \ll \Delta_k^{(s)}(\vartheta), \tag{9}$$

where

$$\Delta_k^{(s)}(\vartheta) = \frac{1}{N} + \frac{1}{m_k} \sum_{0<|\mathbf{a}| \le m_{k-1}} \frac{1}{r(\mathbf{a})} \sum_{c=0}^{m_k-1} \frac{1}{\max\{1, \|c\|_{m_k}\}} \left| \sum_{n=0}^{m_k-1} \mathbf{e}_p\left(\sum_{j=0}^{s-1} a_{j+1} u_{n+j}(\vartheta) \right) \mathbf{e}_{m_k}(cn) \right|.$$

Now,

$$\sum_{\vartheta=0}^{p-1} \Delta_k^{(s)}(\vartheta) = \frac{p}{N} + \frac{1}{m_k} \sum_{0<|\mathbf{a}|\le m_{k-1}} \frac{1}{r(\mathbf{a})} \sum_{c=0}^{m_k-1} \frac{1}{\max\{1, \|c\|_{m_k}\}} \times \sum_{\vartheta=0}^{p-1} \left| \sum_{n=0}^{m_k-1} \mathbf{e}_p\left(\sum_{j=0}^{s-1} a_{j+1} u_{n+j}(\vartheta) \right) \mathbf{e}_{m_k}(cn) \right|$$

$$= \frac{p}{N} + \frac{1}{m_k} \sum_{0<|\mathbf{a}|\le m_{k-1}} \frac{1}{r(\mathbf{a})} \sum_{c=0}^{m_k-1} \frac{1}{\max\{1, \|c\|_{m_k}\}} \times \sum_{\vartheta=0}^{p-1} \left| \sum_{n=0}^{m_k-1} \mathbf{e}_p\left(\sum_{j=0}^{s-1} a_{j+1} \psi^{n+j}(\vartheta) \right) \mathbf{e}_{m_k}(cn) \right|.$$

Applying the Cauchy–Schwarz inequality, from Lemma 1 we derive

$$\sum_{\vartheta=0}^{p-1} \left| \sum_{n=0}^{m_k-1} \mathbf{e}_p\left(\sum_{j=0}^{s-1} a_{j+1} \psi^{n+j}(\vartheta) \right) \mathbf{e}_{m_k}(cn) \right| \ll p^{1/2} A(m_k, p)^{1/2}.$$

Therefore,

$$\sum_{\vartheta=0}^{p-1} \Delta_k^{(s)}(\vartheta) \ll \frac{p}{N} + \frac{p^{1/2} A(m_k, p)^{1/2}}{m_k} \sum_{0<|\mathbf{a}|\le m_{k-1}} \frac{1}{r(\mathbf{a})} \sum_{c=0}^{m_k-1} \frac{1}{\max\{1, \|c\|_{m_k}\}} \ll \frac{p^{1/2} A(m_k, p)^{1/2} (\log m_k)^{s+1}}{m_k},$$

where we used the standard bound for partial sums of the harmonic series in the last step. Thus, for each $k = 1, \ldots, \lceil \log T \rceil$, the inequality

$$\Delta_k^{(s)}(\vartheta) \ge \frac{A(m_k, p)^{1/2} (\log m_k)^{s+1} \log T}{\varepsilon m_k p^{1/2}} = \varepsilon^{-1} B(m_k, p, T) \tag{10}$$

can hold for at most $O(\varepsilon p / \log T)$ values of $\vartheta = 0, 1, \ldots, p-1$. Therefore, the number of $\vartheta = 0, 1, \ldots, p-1$ for which (10) holds for at least one $k = 1, \ldots, \lceil \log T \rceil$ is $O(\varepsilon p)$. For all other ϑ, we get from (9),

$$D_N^{(s)}(\vartheta) \ll \Delta_k^{(s)}(\vartheta) < \varepsilon^{-1} B(m_k, p, T) \ll \varepsilon^{-1} B(N, p, T)$$

for $1 \le N \le T$, where we used $m_k = 2m_{k-1} < 2N$ in the last step. ∎

4. DISCREPANCY BOUND FOR DIGITAL INVERSIVE PSEUDORANDOM NUMBERS

For the generation of digital inversive pseudorandom numbers, we let $q = p^r$ with a (small) prime p and an integer $r \geq 2$. Let $u_0(\vartheta), u_1(\vartheta), \ldots$ be the sequence of elements of $\mathbb{F}_q$ generated by (1) and (2) with the initial value $u_0(\vartheta) = \vartheta \in \mathbb{F}_q$. Then we view $\mathbb{F}_q$ as an r-dimensional vector space over $\mathbb{F}_p$ and we again identify $\mathbb{F}_p$ with the least residue system modulo p. For $n = 0, 1, \ldots$ let

$$(c_n^{(1)}(\vartheta), \ldots, c_n^{(r)}(\vartheta)) \in \mathbb{F}_p^r$$

be the coordinate vector of $u_n(\vartheta) \in \mathbb{F}_q$ relative to a given ordered basis of $\mathbb{F}_q$ over $\mathbb{F}_p$. Now a sequence $x_0(\vartheta), x_1(\vartheta), \ldots$ of *digital inversive pseudorandom numbers* in the interval $[0, 1)$ is defined by

$$x_n(\vartheta) = \sum_{j=1}^{r} c_n^{(j)}(\vartheta) p^{-j} \qquad \text{for } n = 0, 1, \ldots \ .$$

These pseudorandom numbers were introduced by Eichenauer-Herrmann and Niederreiter [8]. It is obvious that if t is the least period of the sequence $u_0(\vartheta), u_1(\vartheta), \ldots$, then the sequence $x_0(\vartheta), x_1(\vartheta), \ldots$ is purely periodic with least period t.

Let $s \geq 1$ be an integer. We denote by $D_N^{(s)}(\vartheta)$ the *s-dimensional discrepancy* of the s-tuples

$$(x_n(\vartheta), x_{n+1}(\vartheta), \ldots, x_{n+s-1}(\vartheta)), \qquad 0 \leq n \leq N-1.$$

We define the number T as in the beginning of Section 2 and put

$$C(N, q, T) = \begin{cases} N^{-1/2} (\log q)^s (\log N + 1) \log (T+1) & \text{if } N \leq q^{1/2}, \\ q^{-1/4} (\log q)^s (\log N + 1) \log (T+1) & \text{if } N > q^{1/2}. \end{cases}$$

THEOREM 4. *Let $s \geq 1$ be an integer and $0 < \varepsilon < 1$. Then for all initial values $\vartheta \in \mathbb{F}_q$, except at most $O(\varepsilon q)$ of them, the discrepancy $D_N^{(s)}(\vartheta)$ of digital inversive pseudorandom numbers satisfies*

$$D_N^{(s)}(\vartheta) \ll \varepsilon^{-1} C(N, q, T) \qquad \textit{for } 1 \leq N \leq T.$$

Proof. We can again assume that $N \geq 2$. For any initial value $\vartheta \in \mathbb{F}_q$, we first proceed as in the proof of [26, Theorem 7]. Let $C_{s \times r}^*(p)$ be the set of all nonzero $s \times r$ matrices whose entries are integers from the interval

$(-p/2, p/2]$. For $H \in C^*_{s\times r}(p)$, let the positive weight $W_p(H)$ be defined as on p. 197 of [26]. Then by [26, Eq. (13)] we have

$$D_N^{(s)}(\vartheta) \ll \frac{1}{q} + \frac{1}{N} \sum_{H \in C^*_{s\times r}(p)} W_p(H) |S_N(H, \vartheta)|$$

with

$$S_N(H, \vartheta) = \sum_{n=0}^{N-1} \chi\left(\sum_{j=1}^{s} \mu_j \psi^{n+j-1}(\vartheta) \right),$$

where $\mu_1, \ldots, \mu_s \in \mathbb{F}_q$ depend on H and are not all 0. Now we proceed in analogy with the proof of Theorem 3. Let $m_v = 2^v$, $v = 0, 1, \ldots$, and define $k \geq 1$ by the condition $m_{k-1} < N \leq m_k$. Then, as in the proof of Theorem 3 we obtain

$$|S_N(H, \vartheta)| \leqslant \sum_{c=0}^{m_k-1} \frac{1}{\max\{1, 2\|c\|_{m_k}\}} \left| \sum_{n=0}^{m_k-1} \chi\left(\sum_{j=1}^{s} \mu_j \psi^{n+j-1}(\vartheta) \right) \mathbf{e}_{m_k}(cn) \right|.$$

It follows that

$$D_N^{(s)}(\vartheta) \ll \Delta_k^{(s)}(\vartheta),$$

where

$$\Delta_k^{(s)}(\vartheta) = \frac{1}{q} + \frac{1}{m_k} \sum_{H \in C^*_{s\times r}(p)} W_p(H) \sum_{c=0}^{m_k-1} \frac{1}{\max\{1, \|c\|_{m_k}\}} \times \left| \sum_{n=0}^{m_k-1} \chi\left(\sum_{j=0}^{s-1} \mu_{j+1} \psi^{n+j}(\vartheta) \right) \mathbf{e}_{m_k}(cn) \right|.$$

Now,

$$\sum_{\vartheta \in \mathbb{F}_q} \Delta_k^{(s)}(\vartheta) = 1 + \frac{1}{m_k} \sum_{H \in C^*_{s\times r}(p)} W_p(H) \sum_{c=0}^{m_k-1} \frac{1}{\max\{1, \|c\|_{m_k}\}} \times \sum_{\vartheta \in \mathbb{F}_q} \left| \sum_{n=0}^{m_k-1} \chi\left(\sum_{j=0}^{s-1} \mu_{j+1} \psi^{n+j}(\vartheta) \right) \mathbf{e}_{m_k}(cn) \right|.$$

From the Cauchy–Schwarz inequality and Lemma 1 we obtain

$$\sum_{\vartheta \in \mathbb{F}_q} \left| \sum_{n=0}^{m_k-1} \chi\left(\sum_{j=0}^{s-1} \mu_{j+1} \psi^{n+j}(\vartheta) \right) \mathbf{e}_{m_k}(cn) \right| \ll q^{1/2} A(m_k, q)^{1/2}.$$

If we note also that

$$\sum_{H \in C_{s \times r}^*(p)} W_p(H) \ll (\log q)^s$$

by [26, Lemma 6], then we get

$$\sum_{\vartheta \in \mathbb{F}_q} \Delta_k^{(s)}(\vartheta) \ll \frac{q^{1/2} A(m_k, q)^{1/2} (\log q)^s \log m_k}{m_k}.$$

The proof is now completed as in Theorem 3. ■

5. REMARKS

Theorems 3 and 4 yield a nontrivial discrepancy bound whenever N is at least of the order of magnitude $(\log p)^{2s+2+\theta}$, respectively $(\log q)^{2s+2+\theta}$, for some $\theta > 0$. We remark that the bound in [14] for inversive congruential pseudorandom numbers, namely

$$D_N^{(s)}(\vartheta) \ll N^{-1/2} p^{1/4} (\log p)^s,$$

which holds for all initial values ϑ and $1 \le N \le t$ where $t \le T$ is the period of the corresponding sequence, is nontrivial only for N at least of the order of magnitude $p^{1/2}(\log p)^{2s+\theta}$. A similar statement holds with regard to the bound

$$D_N^{(s)}(\vartheta) \ll N^{-1/2} q^{1/4} (\log q)^s$$

in [26] for digital inversive pseudorandom numbers. In the case of greatest practical interest, namely when $t = p$ in the inversive congruential method and $t = q$ in the digital inversive method, Theorems 3 and 4 can also be interpreted as discrepancy bounds for "almost all" segments of length N in a given sequence of inversive congruential, respectively digital inversive, pseudorandom numbers.

It should be of interest to apply our technique to some other similar inversive generators such as those of [23, 26, 29–31]; see also the survey [28]. Unfortunately, for another important class of pseudorandom number generators, namely for polynomial generators, our method does not give any significant improvement on the "individual" results of [24].

We remark that our method works for generators modulo a composite number as well. But one should expect weaker results because instead of the very powerful Weil bound which is implicit in the proof of Lemma 1, one will have to use bounds on exponential sums with composite denominator which are essentially weaker; see [15, 16, 32].

REFERENCES

1. W.-S. Chou, The period lengths of inversive pseudorandom vector generations, *Finite Fields Appl.* **1** (1995), 126–132.
2. S. D. Cohen, H. Niederreiter, I. E. Shparlinski, and M. Zieve, Incomplete character sums and a special class of permutations, *J. Théorie des Nombres Bordeaux* **13** (2001), 53–63.
3. M. Drmota and R. F. Tichy, "Sequences, Discrepancies and Applications," Lecture Notes in Mathematics, Vol. 1651, Springer-Verlag, Berlin, 1997.
4. J. Eichenauer and J. Lehn, A non-linear congruential pseudo random number generator, *Statist. Papers* **27** (1986), 315–326.
5. J. Eichenauer-Herrmann and F. Emmerich, Compound inversive congruential pseudorandom numbers: An average-case analysis, *Math. Comput.* **65** (1996), 215–225.
6. J. Eichenauer-Herrmann, F. Emmerich, and G. Larcher, Average discrepancy, hyperplanes, and compound pseudorandom numbers, *Finite Fields Appl.* **3** (1997), 203–218.
7. J. Eichenauer-Herrmann, E. Herrmann, and S. Wegenkittl, A survey of quadratic and inversive congruential pseudorandom numbers, *in* "Monte Carlo and Quasi-Monte Carlo Methods 1996" (H. Niederreiter *et al.*, Eds.), Lecture Notes in Statistics, Vol. 127, pp. 66–97, Springer-Verlag, New York, 1998.
8. J. Eichenauer-Herrmann and H. Niederreiter, Digital inversive pseudorandom numbers, *ACM Trans. Model. Comput. Simul.* **4** (1994), 339–349.
9. M. Flahive and H. Niederreiter, On inversive congruential generators for pseudorandom numbers, *in* "Finite Fields, Coding Theory, and Advances in Communications and Computing" (G.L. Mullen and P.J.-S. Shiue, Eds.), pp. 75–80, Marcel Dekker, New York, 1993.
10. J. B. Friedlander, D. Lieman, and I. E. Shparlinski, On the distribution of the RSA generator, *in* "Sequences and Their Applications" (C. Ding, T. Helleseth, and H. Niederreiter, Eds.), pp. 205–212, Springer-Verlag, London, 1999.
11. J. B. Friedlander and I. E. Shparlinski, On the distribution of the power generator, *Math. Comput.* **70** (2001), 1575–1589.
12. F. Griffin, H. Niederreiter, and I. E. Shparlinski, On the distribution of nonlinear recursive congruential pseudorandom numbers of higher orders, *in* "Applied Algebra, Algebraic Algorithms and Error-Correcting Codes" (M. Fossorier *et al.*, Eds.), Lecture Notes in Computer Science, Vol. 1719, pp. 87–93, Springer-Verlag, Berlin, 1999.
13. J. Gutierrez and D. Gomez-Perez, Iterations of multivariate polynomials and discrepancy of pseudorandom numbers, *in* "Proceedings of the 14th Symp. on Applied Algebra, Algebraic Algorithms and Error-Correcting Codes, 2001, Melbourne," Lecture Notes in Computer Science, Vol. 2227, pp. 192–199, Springer-Verlag, Berlin, 2001.
14. J. Gutierrez, H. Niederreiter, and I. E. Shparlinski, On the multidimensional distribution of inversive congruential pseudorandom numbers in parts of the period, *Monatsh. Math.* **129** (2000), 31–36.
15. D. Ismoilov, Estimates for complete trigonometric sums, *Trudy Mat. Inst. Steklov.* **207** (1994), 153–171 (in Russian).
16. D. Ismoilov, On a method of Hua Loo-Keng of estimating complete trigonometric sums, *Adv. in Math. (China)* **23** (1994), 31–49.
17. R. Lidl and H. Niederreiter, Finite fields and their applications, *in* "Handbook of Algebra" (M. Hazewinkel, Ed.), Vol. 1, pp. 321–363, Elsevier, Amsterdam, 1996.
18. H. Niederreiter, The serial test for congruential pseudorandom numbers generated by inversions, *Math. Comput.* **52** (1989), 135–144.

19. H. Niederreiter, "Random Number Generation and Quasi-Monte Carlo Methods," SIAM, Philadelphia, 1992.
20. H. Niederreiter, Finite fields, pseudorandom numbers, and quasirandom points, *in* "Finite Fields, Coding Theory, and Advances in Communications and Computing" (G. L. Mullen and P.J.-S. Shiue, Eds.), pp. 375–394, Marcel Dekker, New York, 1993.
21. H. Niederreiter, Pseudorandom vector generation by the inversive method, *ACM Trans. Model. Comput. Simul.* **4** (1994), 191–212.
22. H. Niederreiter, New developments in uniform pseudorandom number and vector generation, *in* "Monte Carlo and Quasi-Monte Carlo Methods in Scientific Computing" (H. Niederreiter and P. J.-S. Shiue, Eds.), Lecture Notes in Statistics, Vol. 106, pp. 87–120, Springer-Verlag, New York, 1995.
23. H. Niederreiter, Design and analysis of nonlinear pseudorandom number generators, *in* "Monte Carlo Simulation" (G. I. Schuëller and P. D. Spanos, Eds.), pp. 3–9, A. A. Balkema Publishers, Rotterdam, 2001.
24. H. Niederreiter and I. E. Shparlinski, On the distribution and lattice structure of nonlinear congruential pseudorandom numbers, *Finite Fields Appl.* **5** (1999), 246–253.
25. H. Niederreiter and I. E. Shparlinski, Exponential sums and the distribution of inversive congruential pseudorandom numbers with prime-power modulus, *Acta Arith.* **92** (2000), 89–98.
26. H. Niederreiter and I. E. Shparlinski, On the distribution of pseudorandom numbers and vectors generated by inversive methods, *Appl. Algebra Eng. Comm. Comput.* **10** (2000), 189–202.
27. H. Niederreiter and I. E. Shparlinski, On the distribution of inversive congruential pseudorandom numbers in parts of the period, *Math. Comput.* **70** (2001), 1569–1574.
28. H. Niederreiter and I. E. Shparlinski, Recent advances in the theory of nonlinear pseudorandom number generators, *in* "Monte Carlo and Quasi-Monte Carlo Methods 2000" (K.-T. Fang, F. J. Hickernell, and H. Niederreiter, Eds.), pp. 86–102, Springer-Verlag, Berlin, 2002.
29. H. Niederreiter and A. Winterhof, Incomplete exponential sums over finite fields and their applications to new inversive pseudorandom number generators, *Acta Arith.* **93** (2000), 387–399.
30. H. Niederreiter and A. Winterhof, On the distribution of compound inversive congruential pseudorandom numbers, *Monatsh. Math.* **132** (2001), 35–48.
31. H. Niederreiter and A. Winterhof, On a new class of inversive pseudorandom numbers for parallelized simulation methods, *Period. Math. Hungar.* **42** (2001), 77–87.
32. S. B. Stečkin, An estimate of a complete rational trigonometric sum, *Trudy Mat. Inst. Steklov.* **143** (1977), 188–207 (in Russian).